23.05.25
LANGE NACHT
DER KIRCHEN

Aargauer
Landeskirchen

Anhang 2

Datenbearbeitungsvereinbarung

1. Anbieterinnen und Datenbearbeiterinnen

(a) Die Anbieterinnen und Datenbearbeiterinnen (im Folgenden: Datenbearbeiterinnen) bearbeiten für die Erbringung der im Zusammenarbeits- und Nutzungsvertrag zwischen den Parteien (Vertrag) vereinbarten Leistungen Daten, gegebenenfalls personenbezogene Daten der Nutzerin (vertragsgegenständliche Daten).

(b) Soweit die Datenbearbeiterinnen Daten an Dritte weitergeben, welche letztere für eigene Zwecke bearbeiten dürfen, wird darauf in dieser Datenbearbeitungsvereinbarung und/oder den Beilagen explizit hingewiesen und dies wird von der Nutzerin zur Kenntnis genommen. Die Dritte, die solche Daten erhält und für eigene Zwecke bearbeitet ist die Verantwortliche («Controller») i.S. des Schweizer Bundesgesetzes über den Datenschutz («DSG») und steht für solche eigenen Datenbearbeitungen gegenüber der Nutzerin vollumfänglich in der Pflicht. Die Nutzerin erhält Kontaktdaten solcher allfälliger Dritter in der Datenbearbeitungsvereinbarung und/oder den Beilagen explizit mitgeteilt und darf sich an diese direkt wenden, um ihre zwingenden Betroffenenrechte gemäss DSG geltend zu machen.

(c) Soweit diese Vereinbarung nichts Abweichendes vorsieht, gelten die Bestimmungen des Zusammenarbeitsvertrages.

2. Begriffe

(a) **Kategorien von Personendaten**: Profildaten (wie Vor- und Nachname, Adresse, Telefonnummer, E-Mail-Adresse, Nutzername, Passwort, Zugriffsrechte, IP-Adresse, Fotos) und Nutzungsdaten (wie Interessenprofile, Daten zum Nutzerverhalten, Aktivitätsdaten, Nutzerprofile, Ratings).

(b) **Kreis der betroffenen Personen:** Nutzer des Content Hub (wie die Nutzerin, ihre Angestellten und Beauftragten) und Personen, bezüglich derer die Nutzerin den Datenbearbeiterinnen im Rahmen der Nutzung des Content Hub Daten liefert (wie Vertragspartner, Kunden und andere Personen).

3. Gegenstand und Dauer der Vereinbarung

(a) Der Gegenstand der Datenbearbeitung, ihre Art und ihr Zweck ergeben sich aus dem Zusammenarbeitsvertrag.

(b) Die Datenbearbeitung beginnt mit Unterzeichnung dieser Vereinbarung und endet mit der Beendigung des Zusammenarbeitsvertrags.

(c) Die Nutzerin kann diese Datenbearbeitungsvereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoss der Datenbearbeiterinnen gegen die Bestimmungen dieser Vereinbarung vorliegt, die Datenbearbeiterinnen eine vertragskonforme Weisung der Nutzerin nicht ausführen können oder wollen oder die Datenbearbeiterinnen vertragswidrig die Prüfrechte der Nutzerin verweigern. Bei Kündigung dieser Datenbearbeitungsvereinbarung fällt auch der Zusammenarbeitsvertrag dahin.

4. Stellung der Nutzerin

Für die Zulässigkeit der Erhebung, Bearbeitung und Nutzung der vertragsgegenständlichen Daten einschliesslich Herstellung der erforderlichen Transparenz und für die Erfüllung der gesetzlichen Betroffenenrechte (z.B. Auskunft, Berichtigung oder Löschung) ist die Nutzerin nach den anwendbaren gesetzlichen Bestimmungen verantwortlich. Die Nutzerin stellt sicher, dass die datenschutzrechtlichen Voraussetzungen zwischen der Nutzerin und den betroffenen Personen für das jeweilige Erheben, Bearbeiten und Nutzen der vertragsgegenständlichen Daten nachweisbar vorliegen, insbesondere

- gewährleistet die Nutzerin, dass sie alle erforderlichen Ankündigungen gemäss Vertrag vorgenommen hat oder, wo erforderlich, Einwilligungen ihrer Mitglieder und Partner zur Bekanntgabe ihrer Daten für statistische Bearbeitungszwecke;
- gewährleistet die Nutzerin, dass die von ihr durch die Datenbearbeiterinnen durchgeführte Bearbeitung im Einklang mit den einschlägigen Gesetzen ist; und
- hält die Nutzerin die Datenbearbeiterinnen vollumfänglich schadlos für allfällige von Betroffenen erhobene Drittansprüchen gestützt auf eine angebliche Verletzung der obgenannten Rechtsgrundlagen.

5. Pflichten der Datenbearbeiterinnen

(a) Befolgung von Weisungen:

(i) Die Datenbearbeiterinnen sind verpflichtet, die vertragsgegenständlichen Daten ausschliesslich für die vertragsgemässen Dienstleistungen zu verwenden und bei ihrer Bearbeitung den Weisungen der Nutzerin zu folgen. Vorbehalten bleiben abweichende Pflichten, die sich aus zwingend anwendbarem Recht ergeben und über die die Nutzerin möglichst frühzeitig zu informieren ist, soweit dies rechtlich zulässig ist.

(ii) Das Weisungsrecht der Nutzerin wird durch den Vertrag und die vorliegende Vereinbarung konkretisiert. Darüberhinausgehende Weisungen sind für die Datenbearbeiterinnen nur dann verbindlich, wenn sie zur Einhaltung zwingender datenschutzrechtlicher Anforderungen erforderlich sind.

(iii) Weisungen sind in Textform (d.h. schriftlich oder per E-Mail) zu erteilen, unter Vorbehalt mündlicher Weisung mit folgender Bestätigung in Textform bei Dringlichkeit. Eine Weisung gilt nur dann als verbindlich, wenn deren Erhalt von der zuständigen Empfängerin bestätigt worden ist.

(iv) Die Datenbearbeiterinnen weisen die Nutzerin darauf hin, wenn sie der Ansicht sind, eine Weisung der Nutzerin verstosse gegen Datenschutzvorschriften. Eine Prüfpflicht seitens der Datenbearbeiterinnen besteht jedoch nicht.

(b) **Vertraulichkeit:** Die Datenbearbeiterinnen verpflichten sich, vertragsgegenständliche Daten vertraulich zu behandeln und nur Personen zugänglich zu machen, die für die Erfüllung ihrer Pflichten auf Zugang zu den vertragsgegenständlichen Daten angewiesen sind. Sie stellen sicher, dass alle Personen mit Zugang zu vertragsgegenständlichen Daten einer gesetzlichen oder vertraglichen Vertraulichkeitspflicht unterstehen.

(c) **Ort der Datenbearbeitung:** Die Bearbeitung und Nutzung der vertragsgegenständlichen Daten finden ausschliesslich in der Schweiz statt. Die Bearbeitung von vertragsgegenständlichen Daten ausserhalb dieses Gebietes ist nur mit ausdrücklicher Information der Nutzerin in Textform und in Übereinstimmung mit den anwendbaren gesetzlichen Bestimmungen zulässig. Die Datenbearbeiterinnen verpflichten sich für den Fall einer erlaubten Datenbekanntgabe in einen Staat ohne angemessenes Datenschutzniveau insbesondere, mit dem Empfänger einen Datentransfervertrag auf der Basis der aktuellen EU-Standardvertragsklauseln zu schliessen.

(d) **Rückgabe- und Löschpflicht:** Nach Beendigung des Vertrags haben die Datenbearbeiterinnen der Nutzerin auf deren Begehren alle vertragsgegenständlichen Daten und alle ggf. überlassenen Datenträger herauszugeben. Ansonsten sind die vertragsgegenständlichen Daten unter Vorbehalt entgegenstehender Rechtspflichten endgültig zu löschen.

6. Datensicherheit

Sicherheitsmassnahmen: Die Datenbearbeiterinnen treffen die in Beilage 1 umschriebenen technischen und organisatorischen Massnahmen zum Schutz der vertragsgegenständlichen Daten (Sicherheitsmassnahmen). Die Nutzerin hat die Dienstleistungen und die Sicherheitsmassnahmen geprüft und beurteilt sie als angemessen und ausreichend. Die Datenbearbeiterinnen sind berechtigt, die Sicherheitsmassnahmen anzupassen, sofern das Sicherheitsniveau dabei nicht gesenkt wird.

7. Unterauftragnehmer

(a) **Voraussetzungen:** Für die Erbringung der Leistung können die Datenbearbeiterinnen Unterauftragnehmer beiziehen, sofern die Datenbearbeiterinnen mit dem Unterauftragnehmer eine durchsetzbare Vereinbarung treffen, die inhaltlich der vorliegenden Vereinbarung entspricht. Auf Anfrage ist der Nutzerin der wesentliche Inhalt der entsprechenden Vereinbarung in Kopie zu übermitteln.

(b) **Unterauftragnehmer im Ausland:** Sofern vertragsgegenständliche Daten im Zusammenhang mit dem erlaubten Beizug eines Unterauftragnehmers in einen Staat ohne angemessenes Datenschutzniveau gelangen bzw. von dort zugänglich sind, sind die Datenbearbeiterinnen verpflichtet, vor der ersten Bekanntgabe von vertragsgegenständlichen Daten an den betreffenden Unterauftragnehmer in Übereinstimmung mit dem anwendbaren Datenschutzrecht geeignete Garantien vorzusehen (insb. die anwendbaren EU-Standardvertragsklauseln) und während der gesamten Vertragsdauer aufrechtzuerhalten. Die Nutzerin ist über diese Garantien vorgängig zu informieren.

(c) **Genehmigung:** Eine Liste der bestehenden Unterauftragnehmer mit Zugriff auf vertragsgegenständliche Daten findet sich in Beilage 2. In Beilage 2 sind ebenfalls spezifisch in Bezug auf den jeweiligen Unterauftragnehmer anwendbare Regeln aufgeführt. Vor einer Änderung der Unterauftragnehmerverhältnisse wird die Nutzerin schriftlich oder per E-Mail informiert. Erklärt sie nicht innerhalb von zwei Wochen ebenfalls schriftlich oder per E-Mail aus wichtigen Gründen, dass sie mit der geplanten Änderung nicht einverstanden ist, gilt der betreffende Unterauftragnehmer als genehmigt.

(d) **Dokumentation:** Auf Anfrage übermitteln die Datenbearbeiterinnen der Nutzerin eine Kopie ihrer Vereinbarung(en) mit Unterauftragnehmern (ggf. einschliesslich der geeigneten Garantien), soweit dies erforderlich ist, damit die Nutzerin die Einhaltung dieser Vereinbarung durch die Datenbearbeiterinnen prüfen kann.

(e) **Haftung:** Die Datenbearbeiterinnen haften der Nutzerin für die Einhaltung der Pflichten der Unterauftragnehmer wie für sein eigenes.

8. Prüfrechte

(a) **Prüfrecht:** Die Nutzerin hat das Recht, die Einhaltung der gesetzlichen und vertraglichen Pflichten im Zusammenhang mit der Bearbeitung von vertragsgegenständlichen Daten dieser Vereinbarung durch die Datenbearbeiterinnen zu prüfen. Die Datenbearbeiterinnen sind verpflichtet, bei Prüfungen jeweils angemessen mitzuwirken. Die Parteien einigen sich im Vorfeld über Zeitpunkt, Dauer und Gegenstand der Prüfungen und über anwendbare Sicherheits- und Vertraulichkeitsbestimmungen.

(b) **Externe Prüfstelle:** Die Nutzerin hat das Recht, die Prüfung nach Ziff. 7(a) durch eine externe, fachkundige und zur Vertraulichkeit verpflichtete Stelle durchführen zu lassen. Die Kosten der externen Prüfstelle nach Ziff. 7(a) trägt die Nutzerin.

9. Unterstützung

(a) **Datensicherheit usw.**: Die Datenbearbeiterinnen unterstützen die Nutzerin in angemessener Weise bei der Einhaltung gesetzlicher Pflichten zur Gewährleistung einer angemessenen Datensicherheit.

(b) **Betroffenenrechte:** Soweit ein Betroffener sich im Zusammenhang mit datenschutzrechtlichen Ansprüchen (z.B. mit einem Auskunfts- oder Löschbegehren) an die Datenbearbeiterinnen wendet, leiten die Datenbearbeiterinnen das entsprechende Begehren unverzüglich der Nutzerin weiter. Sie unterstützen die Nutzerin angemessen bei der Bearbeitung solcher Begehren. Dazu gehört bei Bedarf die Unterstützung bei der Zusammenstellung der erforderlichen Daten und Informationen.

(c) **Informationspflicht:** Kontrollhandlungen und andere Massnahmen von Datenschutz-aufsichtsbehörden sind der Nutzerin unverzüglich zu melden, wenn sie die vertrags-gegenständlichen Daten oder für die Bearbeitung von vertragsgegenständlichen Daten verwendete Systeme betreffen.

(d) **Kostenersatz:** Die Datenbearbeiterinnen können Aufwendungen, die durch die in dieser Ziff. 9 vorgesehenen Unterstützungshandlungen verursacht werden, ohne Aufschlag in Rechnung stellen, sofern sich eine entsprechende Pflicht nicht bereits aus dem Vertrag ergibt. Ein Leistungsverweigerungsrecht der Datenbearbeiterinnen für Unterstützungshandlungen i.S.v. Ziff. 9 besteht aber nicht.

10. Haftung

Die Haftung der Parteien untersteht den Bestimmungen des Vertrags.

Beilage 1: Sicherheitsmassnahmen

Die nachfolgende Beschreibung des Status quo der elementaren Massnahmen zum Schutz personenbezogener Daten kann nicht alle existierenden Sicherheitsmassnahmen des Auftragsverarbeiters abdecken. Insbesondere im Rahmen des Datenschutzes und der Datensicherheit ist es auch nicht praktikabel, vertrauliche Massnahmen detailliert zu beschreiben, da der Schutz der Sicherheitsmassnahmen gegen unbefugte Offenlegung mindestens ebenso wichtig ist wie die Sicherheitsmassnahme selbst. Die Umsetzung eines Grossteils dieser Massnahmen liegt wiederum nicht im direkten Einfluss der Heartbeat GmbH, da die Daten auf den Servern von Amazon AWS bzw. Miro Net AG liegen. Zur Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der Daten wurden folgende Vorkehrungen getroffen:

1. Vertraulichkeit

1.1 Eingangskontrolle

Technische oder organisatorische Massnahmen zur Zugangskontrolle, insbesondere betreffend Legitimation von berechtigten Personen:

Das Ziel der Zugangskontrolle ist es, zu verhindern, dass unbefugte Personen physisch Zugang zu solchen Datenverarbeitungsanlagen erhalten, die personenbezogene Daten verarbeiten oder nutzen.

Aufgrund der jeweiligen Sicherheitsanforderungen werden Geschäftsräume und Einrichtungen in verschiedene Sicherheitszonen mit unterschiedlichen Zutrittsberechtigungen unterteilt. Der Zutritt für Mitarbeiter ist nur mit einem verschlüsselten Ausweis mit Foto möglich. Alle anderen Personen haben nur nach vorheriger Anmeldung (z.B. am Haupteingang) Zugang.

1.2 System-Zugriffskontrolle

Technische (Passwortschutz) und organisatorische (Benutzerstammdaten) Massnahmen betreffend Benutzerkennung und Authentifizierung:

Das Ziel der System-Zugriffskontrolle ist es, die unbefugte Nutzung von Datenverarbeitungssystemen, die für die Verarbeitung und Nutzung personenbezogener Daten verwendet werden, zu verhindern.

Die Benutzerstammdaten und der individuelle Identifikationscode jedes Mitarbeiters werden im globalen Kontaktverzeichnis registriert. Der Zugang zu den Datenverarbeitungssystemen ist nur nach Identifizierung und Authentifizierung unter Verwendung des Identifikationscodes und des Passwortes für das jeweilige System möglich. Zusätzliche technische Schutzvorkehrungen werden durch die Benutzung von Firewalls und Proxyserver getroffen. Um die Zugriffskontrolle zu gewährleisten, werden Verschlüsselungstechnologien eingesetzt (z.B. Remote-Zugriff auf das Gesellschafts-Netzwerk via VPN-Tunnel). Die Eignung einer Verschlüsselungstechnologie wird am Schutzzweck gemessen.

1.3 Daten-Zugriffskontrolle

Bedarfsgerechte Strukturierung des Berechtigungskonzeptes und der Datenzugriffsrechte sowie deren Überwachung und Aufzeichnung:

Massnahmen betreffend Daten-Zugriffskontrolle sind darauf auszurichten, dass nur auf solche Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht, und dass personenbezogene Daten während der Verarbeitung, Nutzung und nach der Speicherung dieser Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Der Zugriff auf die für die Erfüllung der jeweiligen Aufgabe notwendigen Daten wird innerhalb der Systeme und Anwendungen durch ein entsprechendes Rollen- und Berechtigungskonzept sichergestellt. Nach dem «need-to-know»-Prinzip hat jede Rolle nur diejenigen Rechte, die für die Erfüllung der von der einzelnen Person durchzuführenden Aufgabe notwendig sind.

Um die Daten-Zugriffskontrolle zu gewährleisten, wird eine Verschlüsselungstechnologie eingesetzt (z.B. Remote-Zugriff auf das Gesellschafts-Netzwerk via VPN-Tunnel). Die Eignung einer Verschlüsselungstechnologie wird am Schutzzweck gemessen.

1.4 Separationskontrolle

Massnahmen betreffend getrennte Verarbeitung (Speichern, Ändern, Löschen und Übertragen) von Daten mit unterschiedlichen Zwecken:

Das Ziel der Separationskontrolle ist es, sicherzustellen, dass Daten, die für verschiedene Zwecke erhoben wurden, getrennt verarbeitet werden können.

Personenbezogene Daten werden nur für interne Zwecke verwendet. Die Mitarbeiter werden instruiert, personenbezogene Daten nur im Rahmen und zum Zweck ihrer Aufgaben (z.B. Erbringung der Dienstleistung) zu erheben, zu verarbeiten und zu nutzen. Auf technischer Ebene werden hierzu die Multi-Client-Fähigkeit, die Trennung von Funktionen sowie die Trennung von Test- und Produktionssystemen genutzt.

1.5 Pseudonymisierung

Massnahmen betreffend Pseudonymisierung von personenbezogenen Daten:

Die Verarbeitung personenbezogener Daten erfolgt in einer solchen Art und Weise, dass die Daten nicht ohne zusätzliche Informationen einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen getrennt aufbewahrt werden und geeigneten technischen und organisatorischen Massnahmen unterliegen.

2. Integrität

2.1 Übertragungskontrolle

Massnahmen betreffend Beförderung, Übermittlung, Übertragung oder Speicherung personenbezogener Daten auf Datenträgern (manuell oder elektronisch) sowie betreffend die anschliessende Überprüfung:

Das Ziel der Übertragungskontrolle ist es, sicherzustellen, dass personenbezogene Daten während der Übermittlung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können und dass überwacht und festgestellt werden kann, an welche Empfänger eine Übermittlung personenbezogener Daten bestimmt ist.

Die Massnahmen, die zur Gewährleistung der Datensicherheit bei Beförderung, Übermittlung und Übertragung personenbezogener Daten sowie sonstiger Daten erforderlich sind, sind in der Datenschutzrichtlinie des Auftragsverarbeiters detailliert beschrieben. In dieser Policy wird die gesamte Verarbeitung von Daten, von der Erstellung dieser Daten bis zu ihrer Löschung, einschliesslich des Umgangs mit diesen Daten gemäss ihrer Klassifizierung, detailliert beschrieben.

Um die Übertragungskontrolle zu gewährleisten, wird eine Verschlüsselungstechnologie eingesetzt (z.B. Remote-Zugriff auf das Gesellschafts-Netzwerk via VPN-Tunnel). Die Eignung einer Verschlüsselungstechnologie wird am Schutzzweck gemessen.

2.2 Dateneingabekontrolle

Massnahmen betreffend anschliessende Überprüfung, ob und von wem Daten eingegeben, verändert oder gelöscht wurden:

Das Ziel der Dateneingabekontrolle ist es, durch geeignete Massnahmen sicherzustellen, dass die Umstände der Dateneingabe rückwirkend überprüft und überwacht werden können.

Systemeingaben werden in Form von Logfiles aufgezeichnet. Auf diese Weise kann zu einem späteren Zeitpunkt überprüft werden, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht wurden.

3. Verfügbarkeits- und Belastbarkeitskontrolle

Massnahmen betreffend Daten-Backup (physikalisch/logisch) und schnelle Wiederherstellung:

Das Ziel der Verfügbarkeitskontrolle und der schnellen Wiederherstellung ist es, sicherzustellen, dass personenbezogene Daten vor unbeabsichtigter Zerstörung und Verlust geschützt sind und schnell wiederhergestellt werden können.

Werden personenbezogene Daten für die Zwecke, für die sie verarbeitet wurden, nicht mehr benötigt, werden sie unverzüglich gelöscht. Es ist zu beachten, dass die personenbezogenen Daten bei jeder Löschung erst einmal nur gesperrt und dann mit einer gewissen Verzögerung endgültig gelöscht werden. Dies geschieht, um versehentliche Löschungen oder mögliche absichtliche Beschädigungen zu vermeiden.

Aus technischen Gründen können Kopien personenbezogener Daten in Sicherungsdateien vorhanden sein und durch Spiegelung von Diensten erstellt werden. Vorbehaltlich der eigenen gesetzlichen Aufbewahrungspflicht des Auftragsverarbeiters werden auch solche Kopien gelöscht – gegebenenfalls mit einer technisch bedingten Verzögerung. Die Verfügbarkeit der Systeme selbst wird gemäss der erforderlichen Sicherheitsstufe durch entsprechende Sicherheitsmassnahmen sichergestellt.

4. Verfahren für die regelmässige Prüfung, Bewertung und Evaluierung

Massnahmen betreffend Datenschutzmanagement, Incident-Response-Management und Datenschutz durch Design und Auftragssteuerung:

Keine Datenverarbeitung durch Dritte ohne entsprechende Weisungen des Verantwortlichen, z.B.: Klare und unmissverständliche vertragliche Vereinbarungen, formalisierte Auftragsverwaltung, strenge Kontrollen bei der Auswahl des Auftragsverarbeiters, Pflicht zur Vorevaluierung, aufsichtsrechtliche Folgekontrollen.

Beilage 2: Unterauftragnehmer

- Heartbeat GmbH, Bahnhofstrasse 102, CH-5000 Aarau
  (Die Heartbeat GmbH arbeitet ihrerseits mit Amazon AWS und MiroNet AG zusammen und ist ihrerseits verpflichtet, mit diesen Dritten adäquate Vertraulichkeits- und Datenbearbeitungsvereinbarungen zu treffen.)
- Für die Datenbearbeitung durch die Heartbeat GmbH gelten die Allgemeinen Geschäftsbedingungen, die mit der Registrierung und dem Zugriff auf das Produkt Flyo von den Nutzerinnen akzeptiert werden. Sie sind hier abrufbar unter https://flyo.cloud/terms.
- Die Datenbearbeiterinnen übernehmen keine Verantwortung für diese Datenbearbeitungen und die Rechte der betroffenen Personen mit Bezug auf diese Bearbeitungen sind direkt an die Heartbeat GmbH, Herrn Stefan Märke (Geschäftsführer) zu richten unter stefan@heartbeat.gmbh.